Available online at www.sciencedirect.com
ScienceDirect
Journal of Symbolic Computation 43 (2008) 27–45
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Universal characteristic decomposition of radical differential ideals☆

Oleg Golubitsky[1]

Ontario Research Centre for Computer Algebra, Department of Computer Science, University of Western Ontario, London, ON, Canada, N6A 5B7

Received 8 May 2006; accepted 19 August 2007
Available online 1 September 2007

Abstract

We call a differential ideal universally characterizable, if it is characterizable w.r.t. any ranking on partial derivatives. We propose a factorization-free algorithm that represents a radical differential ideal as a finite intersection of universally characterizable ideals. The algorithm also constructs a universal characteristic set for each universally characterizable component, i.e., a finite set of differential polynomials that contains a characterizing set of the ideal w.r.t. any ranking. As a part of the proposed algorithm, the following problem of satisfiability by a ranking is efficiently solved: given a finite set of differential polynomials with a derivative selected in each polynomial, determine whether there exists a ranking w.r.t. which the selected derivatives are leading derivatives and, if so, construct such a ranking.

Keywords: Differential algebra; Radical differential ideals; Factorization-free algorithms; Characteristic decomposition; Universal characteristic sets; Differential rankings

1. Introduction

Consider a differential ring of differential polynomials and a radical differential ideal $\{\Sigma\}$ corresponding to a system of polynomial partial differential equations $\Sigma = 0$. By fixing a ranking $\leq$ on partial derivatives (Kolchin, 1973; Rust and Reid, 1997) and computing a characteristic

☆ This work has been presented at ICPSS 2004, at the Symbolic Computation Seminar of North Carolina State University in 2005, and as a poster at ISSAC 2006.

E-mail address: oleg.golubitsky@gmail.com.

[1] Tel.: +1 519 661 4296; fax: +1 519 661 3515.

doi:10.1016/j.jsc.2007.08.003

decomposition of $\{\Sigma\}$ w.r.t. $\leq$ (Boulier et al., 1999; Hubert, 2000), one can solve the membership problem for $\{\Sigma\}$ and study its dimension properties.

The resulting characteristic decomposition, as well as the complexity of its computation, strongly depends on the choice of the ranking. This dependence is well-known for a special case of differential characteristic sets, namely Gröbner bases of polynomial ideals. Indeed, let us restrict ourselves to the case of partial differential ideals generated by linear homogeneous differential polynomials in one differential indeterminate with constant coefficients (such ideals are prime). Then one can take such a differential polynomial and replace all partial derivatives $\frac{\partial^{i_1+\cdots+i_n}u}{\partial^{i_1}x_1\ldots\partial^{i_n}x_n}$ by monomials $y_1^{i_1}\ldots y_n^{i_n}$. A ranking on partial derivatives of u yields an admissible order on monomials in $y_1,\ldots,y_n$. Consider the ideal generated by the resulting polynomials in $y_1,\ldots,y_n$, compute its Gröbner basis, and replace the monomials by the corresponding partial derivatives. The result will be a characteristic set of the prime differential ideal.

It is known that the complexity of computing a Gröbner basis significantly depends on the term order, and generally degree-compatible Gröbner bases are easier to compute. Given the above relationship between Gröbner bases and characteristic sets, it is not surprising that the complexity of computing a characteristic decomposition of a radical differential ideal depends on the chosen ranking and, generally, characteristic decompositions w.r.t. orderly rankings are easier to compute (however, even the choice among the orderly rankings can make a big difference from the efficiency point of view).

The theory of Gröbner bases also provides two concepts which allow us to study the dependence of the basis on the choice of the term order, namely the Gröbner fan and the universal Gröbner basis (Mora and Robbiano, 1988). These concepts have inspired several efficient algorithms, for example:

- the dynamic Buchberger algorithm computes a Gröbner basis when the term order is not given in advance by constructing (Caboara, 1993) or changing (Gritzmann and Sturmfels, 1993; Golubitsky, 2006a) the optimal order dynamically;
- the Gröbner walk method (Collart et al., 1993; Tran, 2000; Fukuda et al., 2007) transforms the Gröbner basis from one order to another, by changing the term order gradually and reducing the problem to several small Gröbner bases.

The objective of this paper is to generalize the concept of universal Gröbner basis to the case of radical differential ideals and give an efficient factorization-free algorithm for computing it. We will discuss potential applications of the proposed concept of universal characteristic decomposition in the Conclusion.

This generalization is threefold.

First, the family of differential rankings is strictly larger than that of term orders. Consequently, the differential Gröbner fan is larger too, yet always finite (which has been shown in Golubitsky (2006b) for prime differential ideals).

Second, the representation of differential rankings is more complex than that of term orders. According to Rust and Reid (1997), every differential ranking can be specified by a finite collection of matrices with real entries. For the purpose of constructing a universal characteristic decomposition we need to solve the inverse problem: given a finite set of differential polynomials with a derivative selected in each polynomial, determine whether there exists a ranking w.r.t. which the selected derivatives are leading derivatives and, if so, construct such a ranking (that is, find any finite representation for it). This problem was formulated in Rust (1998) and, to our knowledge, remained open; we provide an efficient solution for it.

Third, a radical differential ideal may split into several components during the process of characteristic decomposition. If the latter is computed w.r.t. all possible rankings, it is unclear a priori why the process of splitting will always be finite. The proof of termination is based on the Ritt–Raudenbush Basis Theorem (Ritt, 1950) and constitutes the main result of this paper.

2. Basic concepts of differential algebra

Here we give a brief summary of the basic concepts of differential algebra, referring the reader to Ritt (1950), Kolchin (1973) and Kondratieva et al. (1999) for a more complete exposition.

For a set X, denote by X^∞ the free commutative monoid generated by X.

Let R be a commutative ring. A *derivation* over R is a mapping $\delta : R \to R$ which for every $a, b \in R$ satisfies

$$\delta(a+b) = \delta(a) + \delta(b), \qquad \delta(ab) = \delta(a)b + a\delta(b).$$

A *differential ring* is a commutative ring endowed with a finite set of derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$ which commute pairwise. The elements of the commutative monoid $\Theta = \Delta^\infty$ are called *derivative operators*.

Let $U = \{u_1, \ldots, u_n\}$ be a finite set whose elements are called *differential indeterminates*. Derivative operators apply to differential indeterminates yielding *derivatives* θu. Denote by $\Theta U = \{\theta u \mid \theta \in \Theta,\ u \in U\}$ the set of all derivatives.

Let $\mathbb{K}$ be a differential field of characteristic zero. The differential ring of *differential polynomials* $\mathbb{K}\{U\}$ is the ring of polynomials in infinitely many variables $\mathbb{K}[\Theta U]$ endowed with the set of derivations Δ.

A *differential ideal* I of a differential ring R is an ideal of R stable under the action of derivations. For a subset $A \subset R$, $[A]$ denotes the smallest differential ideal containing A.

An ideal I is called *radical*, if $f^k \in I$ implies $f \in I$. The smallest radical differential ideal containing a given set $\Sigma \subset \mathbb{K}\{U\}$ is denoted $\{\Sigma\}$.

A *ranking* is a total order $\le$ on the set of derivatives ΘU such that, for any differential indeterminates $u, v \in U$ and derivative operators $\theta, \theta_1, \theta_2 \in \Theta$, $u \le \theta u$ and $\theta_1 u \le \theta_2 v \iff \theta\theta_1 u \le \theta\theta_2 v$.

A ranking $\le$ on ΘU induces a total lexicographic order $\le_{\mathrm{lex}}$ on the monoid of *differential terms* $(\Theta U)^\infty$.

3. Characteristic sets

Let $\le$ be a ranking, and let $f \in \mathbb{K}\{U\}$, $f \notin \mathbb{K}$. The derivative θu_j of the highest rank present in f is called the *leader* of f (denoted $\mathrm{ld}_\le f$ or $\mathbf{u}_f$ when the ranking is fixed). Let $d = \deg_{\mathbf{u}_f} f$. Then $f = \sum_{j=0}^d g_j \mathbf{u}_f^j$, where $g_0, \ldots, g_d$ are uniquely defined polynomials free of $\mathbf{u}_f$. Differential polynomial $\mathbf{i}_f = \mathbf{i}_\le f = g_d$ is called the *initial* of f, and differential polynomial $\mathbf{s}_f = \sum_{j=1}^d j g_j \mathbf{u}^{j-1}$ is called the *separant* of f. The *rank* of f, denoted $\mathrm{rk}_\le f$, is by definition the differential term $(\mathbf{u}_f)^d$. When a ranking is fixed, we will omit the subscript $\le$ in $\mathrm{ld}_\le f$, $\mathrm{rk}_\le f$, and write $\mathrm{ld}\, f$, $\mathrm{rk}\, f$.

For a set $A \subset \mathbb{K}\{U\}$, the sets of leaders, ranks, initials, and separants of its elements are denoted $\mathrm{ld}_\le A$, $\mathrm{rk}_\le A$, $\mathbf{i}_A$, and $\mathbf{s}_A$, respectively. Let $H_A = \mathbf{i}_A \cup \mathbf{s}_A$.

A ranking on the set of derivatives induces a total order on the set of ranks, if we consider a rank $\mathbf{u}^d$ ($\mathbf{u} \in \Theta U, d > 0$) as a pair $(\mathbf{u}, d)$ and compare such pairs lexicographically.

Let $f, p \in \mathbb{K}\{U\}$, $p \notin \mathbb{K}$. Differential polynomial f is *partially reduced* w.r.t. p, if f is free of all proper derivatives $\theta\mathbf{u}_p$ (i.e. $\theta \neq 1$) of the leader of p. If f is partially reduced w.r.t. p and $\deg_{\mathbf{u}_p} f < \deg_{\mathbf{u}_p} p$, then f is said to be *(fully) reduced* w.r.t. p. A polynomial f is called *reducible* w.r.t. p, if it is not reduced w.r.t. p.

A differential polynomial f is called *reduced w.r.t. a set of differential polynomials* $A \subset \mathbb{K}\{U\}$, if it is reduced w.r.t. every polynomial $p \in A$. A nonempty subset $A \subset \mathbb{K}\{U\}$ is called *autoreduced*, if every $f \in A$ is reduced w.r.t. $A \setminus \{f\}$.

For an autoreduced set A and a differential polynomial f, the *remainder* of f w.r.t. A is defined as a differential polynomial r reduced w.r.t. A, such that $\mathrm{rk}_\leq r \leq \mathrm{rk}_\leq f$ and there exists $h \in H_A^\infty$ satisfying $hf - r \in [A]$. An algorithm for computing a remainder $\mathrm{rem}_\leq(f, A)$ of f w.r.t. A is given in Kolchin (1973, Section 9).

Every autoreduced set is finite (Kolchin, 1973, Chapter I, Section 9). If $A = \{p_1, \ldots, p_k\}$ is an autoreduced set, then any two leaders $\mathbf{u}_{p_i}, \mathbf{u}_{p_j}$ for $1 \leq i \neq j \leq r$ are distinct. We assume that elements of any autoreduced set are arranged in order of increasing rank of their leaders $\mathbf{u}_{p_1} < \mathbf{u}_{p_2} < \cdots < \mathbf{u}_{p_k}$, so we write $A = p_1, \ldots, p_k$.

Let $A = f_1, \ldots, f_k$ and $B = g_1, \ldots, g_l$ be two autoreduced sets. We say that A has *lower rank than* B and write $\mathrm{rk}_\leq A < \mathrm{rk}_\leq B$, if either there exists $j \in \mathbb{N}$ such that $\mathrm{rk}_\leq f_i = \mathrm{rk}_\leq g_i$ $(1 \leq i < j)$ and $\mathrm{rk}_\leq f_j < \mathrm{rk}_\leq g_j$, or $k > l$ and $\mathrm{rk}_\leq f_i = \mathrm{rk}_\leq g_i$ $(1 \leq i \leq l)$. If $k = l$ and $\mathrm{rk}_\leq f_i = \mathrm{rk}_\leq g_i$ $(1 \leq i \leq k)$, then we say that the ranks of sets A and B are equal.

Any nonempty family of autoreduced sets contains an autoreduced set of the lowest rank (Kolchin, 1973, Chapter I, Section 10). For a set $X \subset \mathbb{K}\{U\}$, an autoreduced subset of X of the lowest rank is called a *characteristic set* of X. Clearly, all characteristic sets of X w.r.t. $\leq$ have the same rank. An autoreduced set A is a characteristic set of X if and only if all nonzero elements of X are reducible w.r.t. A.

4. Characteristic decomposition of radical differential ideals

For a differential ideal I and a set of differential polynomials X, the *saturation* of I by X is defined as the following differential ideal:

$$I : X^\infty = \{f \mid \exists s \in X,\ n \in \mathbb{N} \quad s^n f \in I\}.$$

Let $\leq$ be a ranking. A differential ideal I is called *characterizable* w.r.t. $\leq$ (Hubert, 2000, Definition 2.6), if for a characteristic set C of I w.r.t. $\leq$, $I = [C] : H_C^\infty$. In this case, one says that set C *characterizes* I.

A *characteristic decomposition* of a radical differential ideal I is a representation of I as an intersection of characterizable ideals. Given a set of generators Σ of I and a ranking $\leq$, one can apply algorithms from Boulier et al. (1999) and Hubert (2000) to compute a characteristic decomposition of I w.r.t. $\leq$:

$$\{\Sigma\} = \bigcap_{i=1}^{k} J_i, \quad J_i = [C_i] : H_{C_i}^\infty.$$

For each characterizable component J_i, we assume that C_i is its canonical characteristic set. The latter concept was introduced in Boulier et al. (1999, Theorem 6.2) and Boulier and Lemaire (2000, Definition 3, Theorem 3); the construction also follows from Hubert (2003a, Section 5.4) and Hubert (2003b, Theorem 5.5). It has been studied in Golubitsky et al. (2007), where it appears in the following form:

Definition 1. A characteristic set C of a characterizable differential ideal I w.r.t. a ranking $\leq$ is called *canonical* if for all $f \in C$ the following conditions are satisfied:

(1) the initial $\mathbf{i}_f$ depends only on non-leaders $N = \Theta U \setminus \operatorname{ld} C$
(2) f has no factors in $\mathbb{K}[N] \setminus \mathbb{K}$
(3) the leading coefficient of the leading monomial of f w.r.t. the induced lexicographic order $\leq_{\text{lex}}$ on $(\Theta U)^\infty$ is equal to 1.

The canonical characteristic set of a characterizable ideal I can be computed from any other characterizing set of this ideal by inverting the initials (Boulier and Lemaire, 2000, Section 5) or using the remark after (Hubert, 2000, Lemma 3.9). Also, one can check whether two ideals characterizable w.r.t. the same ranking are equal by checking the equality of their canonical characteristic sets.

For our purposes, it is important to ensure that the characteristic sets of the characterizable components are strong (see Definition 2 below). We will show that canonical characteristic sets satisfy this property and use this fact in the proof of termination of the algorithm computing a universal characteristic decomposition of a radical differential ideal.

Definition 2 (*Golubitsky, 2006b*). Let I be a differential ideal, and let $\leq$ be a ranking. Define the **characteristic rank** of I w.r.t. $\leq$, $\operatorname{rkchar}_{\leq} I$, to be equal to the rank of any characteristic set of I w.r.t. $\leq$.

A characteristic set A of an ideal I w.r.t. a ranking $\leq$ is called **strong**, if for all rankings $\leq'$ such that $\operatorname{rkchar}_{\leq'} I = \operatorname{rk}_{\leq} A$, we have $\operatorname{rk}_{\leq'} A = \operatorname{rk}_{\leq} A$.

For example, the characteristic rank of the differential ideal $[u_x + u_y]$ in the differential polynomial ring $\mathbb{K}\{u\}$ with two derivations is equal to $\{u_x\}$ w.r.t. rankings satisfying $u_x > u_y$, and to $\{u_y\}$ w.r.t. rankings satisfying $u_x < u_y$. The set $\{u_x + u_y\}$ is a strong characteristic set of this ideal, since it is autoreduced and its rank equals the characteristic rank of the ideal (w.r.t. any ranking). The set $\{u_{yy}(u_x + u_y)\}$ is a characteristic set of this ideal as well, for rankings satisfying $u_x > u_{yy}$, yet not a strong one. Indeed, the characteristic rank of the ideal w.r.t. such rankings is $\{u_x\}$, and it is not the case that for all rankings $\leq'$ yielding the same characteristic rank of the ideal, the set $\{u_{yy}(u_x + u_y)\}$ will have rank $\{u_x\}$. As a counterexample, take any ranking satisfying $u_y < u_x < u_{yy}$.

The proof of the fact that canonical characteristic sets are strong is based on the following two lemmas. They have been proved in Golubitsky (2006b) for prime differential ideals, and the proofs for characterizable ideals are quite similar, but for the sake of completeness we present them here. Lemma 1 is a simple generalization of Kondratieva and Ovchinnikov (2004, Lemma 1) to the case of characterizable differential ideals.

Lemma 1. *Let C be an autoreduced set characterizing a differential ideal I w.r.t. a ranking $\leq$, and let $f \in I$, $f \notin \mathbb{K}$, be a polynomial such that* $\operatorname{rk}_{\leq} f$ *is reduced w.r.t. C. Then $\mathbf{i}_f \in I$.*

Proof. Since $f \in I$, f is reducible to 0 w.r.t. C and $\leq$. This means that there exist differential polynomials $p_1, \ldots, p_k \in \Theta C$ such that

$$hf \in (p_1, \ldots, p_k),$$

where $h = h_1 \ldots h_k$, $h_i = \mathbf{i}_{p_i} \in H_C$, $\operatorname{rk} p_i \leq \operatorname{rk} f$, $i = 1, \ldots, k$. Moreover, since $\operatorname{rk} f$ is reduced w.r.t. C, $\operatorname{ld} p_i < \operatorname{ld} f$.

Consider f as a polynomial in $t = \operatorname{ld} f$ with coefficients in the ring $R = \mathbb{K}[\Theta U \setminus \{t\}]$:

$$f = \mathbf{i}_f t^d + a_{d-1} t^{d-1} + \cdots + a_0,$$

where $\mathbf{i}_f, a_{d-1}, \ldots, a_0 \in R$. Since $\operatorname{ld} p_i < \operatorname{ld} f$, we have $p_i \in R$, hence $J = (p_1, \ldots, p_k)$ is an ideal in R. Now, if $(p_1, \ldots, p_k)$ is considered as an ideal in $R[t]$, then every element of this ideal admits a unique representation of the form $a_l t^l + \cdots + a_0$, where $a_i \in J$, $i = 0, \ldots, l$. In particular,

$$hf = h\mathbf{i}_f t^d + ha_{d-1} t^{d-1} + \cdots + ha_0$$

is such a representation for $hf \in J$ (note that $h \in R$, since $h_i = \mathbf{i}_{p_i}$ and $p_i \in R$, $i = 1, \ldots, k$). This implies that $h\mathbf{i}_f \in J$. Therefore $h\mathbf{i}_f \in I$, but since $I = [C] : H_C^\infty$ and $h \in H_C^\infty$, we obtain $\mathbf{i}_f \in I$. $\square$

For a polynomial f, denote by $\operatorname{allrk}(f)$ the set of its ranks w.r.t. all possible rankings; for every $t \in \operatorname{allrk}(f)$, $\mathbf{i}_t f$ denotes the initial of f w.r.t. a ranking $\leq$ such that $t = \operatorname{rk}_\leq f$.

Lemma 2. *Let C be a characteristic set of a characterizable differential ideal I w.r.t. ranking $\leq$ satisfying the following condition:*

$$\forall\ f \in C \ \ \forall\ t \in \operatorname{allrk}(f) \quad \mathbf{i}_t f \notin I.$$

Then C is strong.

Proof. Suppose that C is not strong. Then, according to Definition 2, there exists a ranking $\leq'$ such that $\operatorname{rkchar}_{\leq'} I = \operatorname{rk}_\leq C$ but $\operatorname{rk}_{\leq'} C \neq \operatorname{rk}_\leq C$. The latter implies that there exists a polynomial $f \in C$ such that $\operatorname{rk}_{\leq'} f \neq \operatorname{rk}_\leq f$, whence $\operatorname{rk}_{\leq'} f < \operatorname{rk}_\leq f$.

Let C' be a characteristic set of I w.r.t. $\leq'$. Suppose first that $\operatorname{rk}_{\leq'} f$ is reducible w.r.t. a polynomial $g \in C'$ and $\leq'$. Then $\operatorname{rk}_{\leq'} f$ is reducible w.r.t. $\operatorname{rk}_{\leq'} g$, which implies that $\operatorname{rk}_{\leq'} g \leq \operatorname{rk}_{\leq'} f$.

Since $\operatorname{rkchar}_{\leq'} I = \operatorname{rk}_{\leq'} C' = \operatorname{rk}_\leq C$, there exists a polynomial $p \in C$ such that $\operatorname{rk}_\leq p = \operatorname{rk}_{\leq'} g$. Then $p \neq f$, since

$$\operatorname{rk}_\leq p = \operatorname{rk}_{\leq'} g \leq \operatorname{rk}_{\leq'} f < \operatorname{rk}_\leq f.$$

So, we have obtained that $\operatorname{rk}_{\leq'} f$ is reducible w.r.t. $\operatorname{rk}_\leq p$, hence f is reducible w.r.t. p and $\leq$. This contradicts the fact that f and p are distinct elements of the autoreduced set C.

Therefore, $\operatorname{rk}_{\leq'} f$ is reduced w.r.t. C' and $\leq'$. Now, given that $f \in I$, Lemma 1 implies that the initial of f w.r.t. $\leq'$ belongs to I. This contradicts the assumption

$$\forall\ f \in C \ \ \forall\ t \in \operatorname{allrk}(f) \quad \mathbf{i}_t f \notin I.$$

Thus, C is strong. $\square$

Theorem 1. *The canonical characteristic set of a characterizable differential ideal I w.r.t. ranking $\leq$ is strong.*

Proof. Let C be the canonical characteristic set of I w.r.t. $\leq$, let $f \in C$, and let $t \in \operatorname{allrk}(f)$. Suppose that $\mathbf{i}_t f \in I$. Then, since $\mathbf{i}_t f \neq 0$, $\mathbf{i}_t f$ is reducible w.r.t. C. Since C is autoreduced, f is reduced w.r.t. $C \setminus \{f\}$, hence so is $\mathbf{i}_t f$. Thus, $\mathbf{i}_t(f)$ is reducible w.r.t. f. The latter implies that

$$\operatorname{rk}_\leq \mathbf{i}_t f = \operatorname{rk}_\leq f, \tag{1}$$

since it is always the case that $\operatorname{rk}_\leq \mathbf{i}_t f \leq \operatorname{rk}_\leq f$.

Note that set $C' = C \setminus \{f\} \cup \{\mathbf{i}_t(f)\}$ is also a characteristic set of I w.r.t. $\leq$. Since f is an element of the canonical characteristic set, the initial of f w.r.t. $\leq$ belongs to the ring $\mathbb{K}[N]$, where $N = \Theta U \setminus \mathrm{ld}_{\leq} C$. Now equality (1) implies that the initial of $\mathbf{i}_t f$ w.r.t. $\leq$ also belongs to $\mathbb{K}[N]$. Thus, the initials of C' w.r.t. $\leq$ are in $\mathbb{K}[N]$. Moreover, we have

$$\mathbf{i}_{\mathbf{i}_t f} <_{\mathrm{lex}} \mathbf{i}_t f.$$

The latter contradicts Golubitsky et al. (2007, Proposition 3), according to which the initials of the elements of the canonical characteristic set are lexicographically less than or equal to the initials of the corresponding elements of any other characteristic set, whose initials do not depend on leaders.

Thus, $\mathbf{i}_t f \notin I$ and, by Lemma 2, set C is strong. □

5. Universal characteristic decomposition

Let C be an autoreduced set characterizing a differential ideal I w.r.t. a ranking $\leq$, and let $\leq'$ be another ranking. Let CharacteristicDecomposition(C,$\leq$,$\leq'$) be any factorization-free algorithm that computes a characteristic decomposition of I w.r.t. $\leq'$, in which every characterizable component is represented by its canonical characteristic set.

Definition 3. A differential ideal I is called **universally characterizable**, if it is characterizable w.r.t. any ranking.

In this case, a **universal characteristic set** of I is defined as a finite subset $C \subset I$, such that for any ranking $\leq$, there exists an autoreduced subset $C_{\leq} \subset C$ which characterizes I w.r.t. $\leq$.

Every prime differential ideal is universally characterizable (Golubitsky, 2006b). The converse is not true: for example, radical ideal $(x^2 + x) \subset \mathbb{Q}[x]$ is universally characterizable, $\{x^2 + x\}$ being its characteristic set w.r.t. the only ranking that is possible in this case, but it is not prime.

Definition 4. For a radical differential ideal I, its **universal characteristic decomposition** is a representation of I as a finite intersection of universally characterizable differential ideals.

We propose a factorization-free algorithm (Algorithm 1) that, given a characteristic decomposition of a radical differential ideal w.r.t. a ranking $\leq$, computes a universal characteristic decomposition of this ideal. Moreover, for each universally characterizable component, the algorithm computes the corresponding universal characteristic set.

In order to check the condition of the **while**-loop in algorithm UniversalCharacteristicDecomposition, we have to solve the following problem: given a finite set of polynomials C and a family of autoreduced sets of ranks R, determine whether there exists a ranking $\leq'$ such that $\mathrm{rkchar}_{\leq'} C \notin R$. Since C is finite, one can try all possible selections of leaders in C, which are consistent with a ranking on partial derivatives. For example, if $f = u_{xx} + u_{xy} + u_{yy}$, then there exist rankings which select u_{xx} and u_{yy} as leaders of f, but u_{xy} is not a leader of f w.r.t. any ranking. For every selection of leaders in C that is consistent with a ranking, we can construct such ranking $\leq$ and check whether $\mathrm{rkchar}_{\leq} C \in R$.

Therefore, we arrive at a general problem of determining whether a given selection of leaders in a finite set of differential polynomials is consistent with a ranking. The `diffalg` package of Maple 10 contains a subroutine (which is embedded in the procedure for specification of differential rings) that, given a finite set of polynomials with selected derivatives, determines

Algorithm 1 UniversalCharacteristicDecomposition($\mathbf{C}$, $\leq$)

Input: Characteristic decomposition $\mathbf{C}$ of a radical ideal I w.r.t. $\leq$

Output: Universal characteristic decomposition of I

$\mathbf{U} := \{(C, \{\mathrm{rk}_{\leq} C\}) \mid C \in \mathbf{C}\}$
while $\exists$ ranking $\leq'$ s.t. $\{(C, R) \in \mathbf{U} \mid \mathrm{rkchar}_{\leq'} C \notin R\} \neq \emptyset$ **do**
  Take any such ranking $\leq'$
  $\mathbf{V} := \{(C, R) \in \mathbf{U} \mid \mathrm{rkchar}_{\leq'} C \notin R\}$
  $\mathbf{U} := \mathbf{U} \setminus \mathbf{V}$
  for $(C, R) \in \mathbf{V}$ **do**
    $\mathbf{C}' = C'_1, \ldots, C'_p :=$CharacteristicDecomposition(C,$\leq$,$\leq'$)
    $C' := \varnothing, \quad \mathbf{D}' := \varnothing$
    for $C'_i \in \mathbf{C}'$ **do**
      $\mathbf{D} :=$CharacteristicDecomposition(C'_i,$\leq'$,$\leq$)
      if $C \in \mathbf{D}$ **then** $C' := C'_i$
        else $\mathbf{D}' := \mathbf{D}' \cup \bigcup_{D \in \mathbf{D}}$ CharacteristicDecomposition(D, $\leq$, $\leq'$)
      end if
    end for
    if $C' \neq \varnothing$
      then $\mathbf{U} := \mathbf{U} \cup \{(C \cup C', R \cup \{\mathrm{rk}_{\leq'} C'\})\}$
      else $\mathbf{U} := \mathbf{U} \cup \{(D', \{\mathrm{rk}_{\leq'} D'\}) \mid D' \in \mathbf{D}'\}$
    end if
  end for
end while
return U
end

whether there exists a ranking consistent with this selection and, if so, constructs such a ranking. The subroutine applies to a certain subfamily of Riquier rankings which can be efficiently handled by the simplex method.[2] For general (not necessarily Riquier) rankings, we solve this problem in the next section.

Proposition 1. *Algorithm* UniversalCharacteristicDecomposition *is correct, i.e., it returns a universal characteristic decomposition of the ideal I.*

Proof. (1) In each pair $(C, R) \in \mathbf{U}$, the first component C is a set of differential polynomials and the second component R is a family of sets of ranks satisfying the following property: There exists a characterizable ideal $J_{(C,R)} \supseteq I$ which, for each $r \in R$, is characterized by a subset $C_r \subset C$ w.r.t. a ranking $\leq'$ satisfying

$$\mathrm{rkchar}_{\leq'} J = \mathrm{rkchar}_{\leq'} C = \mathrm{rk}_{\leq'} C_r = r.$$

(2) The invariant of the **while**-loop is

$$I = \bigcap_{(C,R) \in \mathbf{U}} J_{(C,R)}.$$

[2] The author is grateful to the referee for pointing out that, for efficiency reasons, not all Riquier rankings are checked by the subroutine in `diffalg`.

(3) At the exit from the **while**-loop, the ideal $J_{(C,R)}$ corresponding to any pair $(C, R) \in \mathbf{U}$ is universally characterizable with the universal characteristic set C. Indeed, we exit from the **while**-loop when for any ranking $\leq'$, there exists $r \in R$ such that

$$\operatorname{rkchar}_{\leq'} J_{(C,R)} = \operatorname{rkchar}_{\leq'} C = r. \quad \square$$

The proof of termination involves the following simple

Lemma 3. *There exist no infinitely growing chains of characterizable ideals of the form $I_1 \subsetneq I_2 \subsetneq \ldots$.*

Proof. According to Hubert (2000, Theorem 4.4), characterizable ideals are radical. Due to the Basis Theorem (Kolchin, 1973, Section III.4), there exist no infinitely growing chains of radical differential ideals. $\square$

Proposition 2. *Algorithm* UniversalCharacteristicDecomposition *terminates.*

Proof. Let $(C, R) \in \mathbf{V}$ be a component considered in line 6 of the algorithm corresponding to a characterizable ideal $J = J_{(C,R)}$ w.r.t. ranking $\leq$. Let $\mathbf{C}' = C'_1, \ldots, C'_p$ be the characteristic decomposition of J w.r.t. $\leq'$ computed in line 7. Two cases are possible: either $J = [C'_i] : H^\infty_{C'_i}$ for some $i \in \{1, \ldots, p\}$, or for all i, $J \subsetneq [C'_i] : H^\infty_{C'_i}$.

One could try to distinguish between these two cases by checking equality of two differential ideals that are characterizable w.r.t. different rankings. To our knowledge, the problem of checking equality of such ideals is open. Here we use a trick (see below), which replaces this problem by the problem of checking equality of two ideals that are characterizable w.r.t. the same ranking. The latter can be done by checking whether their canonical characteristic sets are equal.

The trick corresponds to lines 9–14 of the algorithm. Consider a characteristic decomposition $\mathbf{D}$ of each ideal $[C'_i] : H^\infty_{C'_i}$ w.r.t. $\leq$ computed in line 10. If one of the components $[D] : H^\infty_D$ in $\mathbf{D}$ coincides with J (this condition is verified in the **if**-statement, line 11), then inclusions $J \subseteq [C'_i] : H^\infty_{C'_i} \subseteq [D] : H^\infty_D$ imply that $J = [C'_i] : H^\infty_{C'_i}$. The latter means that J is characterized w.r.t. $\leq'$ by the characteristic set C'_i. In such a case, we add C'_i to C and $\operatorname{rk}_{\leq'} C'_i$ to R (line 16). Note that, according to the condition of the **while**-loop, $\operatorname{rk}_{\leq'} C'_i \notin R$ before we add it. If, on the other hand, none of the components in $\mathbf{D}$ coincides with J, then all components in $\mathbf{D}$ strictly contain J. Hence, so do all components in $\mathbf{D}'$ (line 12), which are added to $\mathbf{U}$ in line 17.

To summarize, a single iteration of the **while**-loop replaces each component (C, R) taken from $\mathbf{U}$ in lines 4, 5 by either a single component (C', R'), where R' strictly contains R (line 16), or a set of components whose ideals strictly contain $J_{(C,R)}$ (line 17). Lemma 3 ensures that, after a finite number of iterations of the **while**-loop, the characterizable components will stop splitting. At this point all components in $\mathbf{U}$ correspond to universally characterizable ideals. Therefore, it remains to show that the computation of their universal characteristic sets is completed in finitely many steps. To illustrate the performance of the **while**-loop after the stabilization of all components, take a $(C, R) \in \mathbf{U}$ and rewrite the **while**-loop for this particular component:

while $\exists \ \leq'$ s.t. $\operatorname{rkchar}_{\leq'} C \notin R$ **do**
  Take any such ranking $\leq'$
  C' :=CanonicalCharacteristicSet(C,$\leq$,$\leq'$)
  $C := C \cup C'$
  $R := R \cup \{\operatorname{rk}_{\leq'} C'\}$
end while

In this algorithm, line 3 corresponds to lines 7–14 of algorithm UniversalCharacteristicDecomposition, where $C' \neq \varnothing$, since the component has stabilized. According to Theorem 1, the above loop has the following invariant: for every set of ranks $r \in R$, C contains a strong characteristic subset whose rank is r w.r.t. some ranking. Thus, condition $\mathrm{rkchar}_{\leq'} C \notin R$ implies that $\mathrm{rk}_{\leq'} C' \notin R$. Now termination of the **while**-loop follows from

Theorem 2 (*Golubitsky, 2006b, Theorem 4*). *The set of ranks of characteristic sets of any differential ideal I w.r.t. all possible rankings is finite.* □

6. Examples

Let us illustrate the proposed algorithm on two examples. The first is an example of an algebraic ideal that is characterizable but not universally characterizable; the algorithm computes its universal characteristic decomposition. The second is an example of a partial differential ideal that is universally characterizable, but not obviously such. Given the generators of this ideal and a particular ranking (chosen arbitrarily), the Rosenfeld–Gröbner algorithm will return two components. The computation of universal characteristic decomposition shows that one of these components is redundant, while the other, and hence the whole ideal, is universally characterizable. This computation also exhibits the ranking for which the Rosenfeld–Gröbner computes an irredundant characteristic decomposition.

Example 1. Consider the ideal $I = (y^3 - y, 2x - y^2 + 2)$ in $\mathbb{Q}[x, y]$ (this example is borrowed from Hubert (2000)). With respect to the ranking $x > y$, this ideal is characterized by its generating set (Hubert, 2000, Example 3.6). However, the characteristic set $C = \{y^3 - y, 2x - y^2 + 2\}$ is not universal, since w.r.t. ranking $x < y$ the characteristic set of C is $\{2x - y^2 + 2\}$, which is not a characteristic set of I. A characteristic decomposition of I w.r.t. ranking $x < y$ has two characterizable components:

$$I = (2x + 1, 2y^2 - 1) \cap (x + 1, y).$$

Clearly, characteristic sets $\{2x+1, 2y^2-1\}$ and $\{x+1, y\}$ are universal (any ranking will select the same leaders in their elements), hence we have obtained a universal characteristic decomposition of I. In this particular case, the decomposition turns out to be irredundant, and the universal characteristic sets of the characterizable components are minimal.

Example 2. Consider the ideal $I = [u_x - v, u_y - uv]$ in $\mathbb{Q}\{u, v\}$ with two derivations $\delta_x = \partial/\partial x,\ \delta_y = \partial/\partial y$.

Fix an elimination ranking $\leq_1$ such that:

- $\theta u <_1 \theta' v$ for all θ, θ'
- $\delta_x^i \delta_y^j u \leq_1 \delta_x^{i'} \delta_y^{j'} u$ iff $i + j \leq i' + j'$ or $i + j = i' + j'$ and $i \leq i'$.
- $\delta_x^i \delta_y^j v \leq_1 \delta_x^{i'} \delta_y^{y'} v$ iff $i + j \leq i' + j'$ or $i + j = i' + j'$ and $i \leq i'$.

Compute a characteristic decomposition of I w.r.t. $\leq_1$. The Rosenfeld–Gröbner algorithm from the `diffalg` package in Maple 10 returns two characterizable components, whose characteristic sets are:

$$C_1 = \{u\underline{u_x} - u_y,\ u\underline{v} - u_y\}, \quad C_2 = \{u, v\}$$

(the leading derivatives w.r.t. $\leq_1$ are underlined, and the elements of characteristic sets are sorted by increasing rank).

There arises a question whether the second component is redundant, i.e., whether $u = v = 0$ is a zero of the differential ideal $[C_1] : H_{C_1}^{\infty}$. This is an instance of the Ritt problem (Kolchin, 1973, Section IV.16), which is open. In a moment we will see that the computation of the universal characteristic decomposition of I reveals the fact that the second component is redundant and the first one (i.e., the ideal I) is universally characterizable.

Following Algorithm UniversalCharacteristicDecomposition (line 3), choose a ranking $\leq'$ such that $\mathrm{rkchar}_{\leq'} C_1 \neq \{u_x, v\}$. We can take $\leq' = \leq_2$, where $\theta u >_2 \theta' v$ for all θ, θ', and the derivatives of the same differential indeterminate are compared w.r.t. $\leq_2$ as w.r.t. $\leq_1$. Then

$$\mathrm{rkchar}_{\leq_2} C_1 = \{u_x, u_y\} \neq \{u_x, v\}.$$

Compute a characteristic decomposition of $[C_1] : H_{C_1}^{\infty}$ w.r.t. $\leq_2$ (line 7). The Rosenfeld–Gröbner algorithm returns two components whose characteristic sets are:

$$\begin{aligned} C_1' = \{ & (v_y - v^2)\underline{v_{xy}} - v_x v_{yy} + v v_x (3v_y - v^2),\ (v_y - v^2)^2 \underline{v_{xx}} - v_x^2 v_{yy} \\ & + 2 v v_x^2 (3 v_y - 2v^2),\ v_x \underline{u} - (v_y - v^2)\} \\ C_2' = \{ & \underline{v_y} - v^2,\ v_x,\ \underline{u_y} - uv,\ \underline{u_x} - v\}. \end{aligned}$$

Our algorithm then, for each of the above two components, computes its characteristic decomposition w.r.t. $\leq_1$ (line 10) and checks whether any of these decompositions contain a component equal to $[C_1] : H_{C_1}^{\infty}$ (line 11).

For $[C_1'] : H_{C_1'}^{\infty}$, the Rosenfeld–Gröbner algorithm produces a single component w.r.t. $\leq_1$, whose characteristic set coincides with C_1. This implies that $[C_1] : H_{C_1}^{\infty} = [C_1'] : H_{C_1'}^{\infty}$, whence $[C_2'] : H_{C_2'}^{\infty}$ is a redundant component.

Our algorithm proceeds by forming the union $C_1 \cup C_1'$ (line 16) and choosing a ranking $\leq_3$ (line 3) such that $\mathrm{rkchar}_{\leq_3}(C_1 \cup C_1')$ is not among the ranks seen before, i.e. $\{u_x, v\}$ and $\{v_{xy}, v_{xx}, u\}$. We can take the following $\leq_3$:

- $\theta u <_3 \theta' v$ for all θ, θ'
- $\delta_x^i \delta_y^j u \leq_3 \delta_x^{i'} \delta_y^{y'} u$ iff $i + j \leq i' + j'$ or $i + j = i' + j'$ and $j \leq j'$.
- $\delta_x^i \delta_y^j v \leq_3 \delta_x^{i'} \delta_y^{y'} v$ iff $i + j \leq i' + j'$ or $i + j = i' + j'$ and $j \leq j'$.

The computation of the characteristic decomposition of $[C_1] : H_{C_1}^{\infty}$ w.r.t. $\leq_3$ yields one component with the characteristic set

$$C_1'' = \{\underline{u_y} - u u_x,\ \underline{v} - u_x\}.$$

Computing the characteristic decomposition of $[C_1''] : H_{C_1''}$ w.r.t. $\leq_1$ yields two components with characteristic sets C_1 and $\{u, v\}$, respectively. This proves two facts: that $[C_1] : H_{C_1}^{\infty} = [C_1''] : H_{C_1''}$ and that the component $\{u, v\}$ is redundant. Note also that $u = v = 0$ is a regular zero of C_1'' and, if the Rosenfeld–Gröbner algorithm is applied to the generators of I and $\leq_3$, it will return the single characterizable component C_1''.

Therefore, the algorithm forms the union $C_1 \cup C_1' \cup C_1''$ (line 16). Choose a ranking $\leq_4$ such that $\mathrm{rkchar}_{\leq_4}(C_1 \cup C_1' \cup C_1'')$ is not among $\{u_x, v\}$, $\{v_{xy}, v_{xx}, u\}$, and $\{u_y, v\}$: let $\theta u >_4 \theta' v$ for all θ, θ' and the derivatives of the same differential indeterminate be compared as w.r.t. $\leq_3$. The characteristic decomposition of $[C_1] : H_{C_1}^{\infty}$ w.r.t. $\leq_4$ has two components, the first of which has characteristic set

$$\begin{aligned} C_1''' = \{ & v_x \underline{v_{xy}} - (v_y - v^2)v_{xx} - 3vv_x^2,\ v_x^2\underline{v_{yy}} - (v_y - v^2)^2 v_{xx} \\ & - 2vv_x^2(3v_y - 2v^2),\ v_x\underline{u} - (v_y - v^2)\} \end{aligned}$$

and is proved to be equal to $[C_1] : H_{C_1}^{\infty}$ by computing its characteristic decomposition w.r.t. $\leq_1$ and finding that it consists of a single component whose characteristic set is C_1. Thus we know that the second component is redundant and proceed to forming the union $C_1 \cup C_1' \cup C_1'' \cup C_1'''$.

Repeat the procedure for two more orderly rankings, $\leq_5$ and $\leq_6$, which, given two derivatives, first compare their orders, then for θ, θ' of the same order, set $\theta u > \theta v$, where $>$ is $>_5$ or $>_6$ and, finally, resolve the comparisons between derivatives of the same order and the same differential indeterminate $w \in \{u, v\}$ as follows:

- $\delta_x^i \delta_y^j w \leq_5 \delta_x^{i'} \delta_y^{j'} w$ iff $i \leq i'$
- $\delta_x^i \delta_y^j w \leq_6 \delta_x^{i'} \delta_y^{j'} w$ iff $j \leq j'$.

This will yield two more characteristic sets:

$$\begin{aligned} C_1'''' &= \{u\underline{v_x} - v_y + v^2,\ \underline{u_y} - uv,\ \underline{u_x} - v\} \\ C_1''''' &= \{\underline{v_y} - uv_x - v^2,\ \underline{u_x} - v,\ \underline{u_y} - uv\} \end{aligned}$$

and the union $\bar{C} = C_1 \cup C_1' \cup C_1'' \cup C_1''' \cup C_1'''' \cup C_1'''''$ consisting of the following eight polynomials will be formed:

$$\begin{aligned} & uu_x - u_y \\ & uv - u_y \\ & (v_y - v^2)v_{xy} - v_x v_{yy} + vv_x(3v_y - v^2) \\ & (v_y - v^2)^2 v_{xx} - v_x^2 v_{yy} + 2vv_x^2(3v_y - 2v^2) \\ & v_x u - (v_y - v^2) \\ & v - u_x \\ & v_x v_{xy} - (v_y - v^2)v_{xx} - 3vv_x^2 \\ & v_x^2 v_{yy} - (v_y - v^2)^2 v_{xx} - 2vv_x^2(3v_y - 2v^2). \end{aligned}$$

Note that the last two characteristic sets do not add any new polynomials to the union, but they do add new characteristic ranks of the ideal. Thus, the ideal admits six possible characteristic ranks w.r.t. the above six rankings $\leq_1, \ldots, \leq_6$:

$$\{u_x, v\},\ \{v_{xy}, v_{xx}, u\},\ \{u_y, v\},\ \{v_{xy}, v_{yy}, u\}, \{v_x, u_y, u_x\}, \{v_y, u_x, u_y\}.$$

One can show, by exhaustively trying all possible selections of leaders of polynomials in $\bar{C}$, that for any ranking, the characteristic rank of $\bar{C}$ will be one of the above six.[3] Thus, $\bar{C}$ is a universal characteristic set of I, whence I is universally characterizable.

7. Satisfiability by differential rankings

The following problem has to be solved by Algorithm UniversalCharacteristicDecomposition: given a finite set of differential polynomials with selected derivatives, determine whether this selection is consistent with a ranking and, if so, construct such a ranking. As is mentioned in Rust (1998), this problem reduces to the following one, which we call *the problem of satisfiability by*

[3] We omit the details of this procedure, as it will be the topic of the next section.

a ranking: given a finite relation $A \subset \Theta U \times \Theta U$, determine whether it is contained in a ranking and, if so, construct any such ranking.

The problem clearly requires a representation of rankings. Different ways of representing a ranking are proposed in Carrà Ferro and Sit (1994) and Rust and Reid (1997).

Following the notation in these articles, we observe that partial derivatives correspond to elements of the set $\mathbb{N}^m \times \mathbb{N}_n$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N}_n = \{1, 2, \ldots, n\}$, via the following mapping $\phi : \Theta U \to \mathbb{N}^{m+n}$:

$$\phi : \delta_1^{i_1} \ldots \delta_m^{i_m} u_j \mapsto \left(i_1, \ldots, i_m, 0, \ldots, \overset{(m+j)}{1}, \ldots, 0\right)^{\mathrm{T}}$$

(here $\vec{x}^{\mathrm{T}}$ denotes the transposed vector $\vec{x}$). Thus, we can equivalently speak of rankings on $\mathbb{N}^m \times \mathbb{N}_n$.

According to Carrà Ferro and Sit (1994, Proposition 1.4), every such ranking uniquely extends to a ranking $\leq$ on $\mathbb{Z}^m \times \mathbb{N}_n$. The latter uniquely induces a family of sets

$$A_{ij} = \{a \in \mathbb{Z}^m \mid (a, i) \leq (0, j)\},$$

where $1 \leq i, j \leq n$, called *cuts*. These cuts are interrelated via the axioms of a transitive family (Carrà Ferro and Sit, 1994, Definition 3.9). Vice versa, according to Carrà Ferro and Sit (1994, Theorem 3.10), every transitive family of cuts induces a unique ranking on $\mathbb{Z}^m \times \mathbb{N}_n$.

Using Carrà Ferro and Sit (1994, Theorem 7.3), any cut of $\mathbb{Z}^m$ can be described by a real-valued matrix and a real vector, though such description is not unique. Thus, every ranking can be specified by finitely many real matrices and vectors (or, in other words, in terms of linear constraints). For our purposes, however, this description of rankings is incomplete, since we do not know how to check whether a given family of cuts, where each cut is specified by linear constraints, is transitive. In Carrà Ferro and Sit (1994), a complete description of transitive families of cuts is given for cuts in $\mathbb{R}^m \times \mathbb{N}_n$; the case of $\mathbb{Z}^m \times \mathbb{N}_n$ is formulated as an open problem, whose solution depends on whether every ranking on $\mathbb{Z}^m \times \mathbb{N}_n$ can be extended to a ranking on $\mathbb{R}^m \times \mathbb{N}_n$.

A classification of rankings on partial derivatives, or equivalently on $\mathbb{Z}^m \times \mathbb{N}_n$, which can be used directly for our purposes, is given in Rust and Reid (1997) (see also Rust (1998)). It is shown that every ranking is a pre-ranking of type $\leq n$, where pre-rankings of type 1 are Riquier pre-rankings; pre-rankings of higher types are defined inductively and can be thought of as finite rooted trees, whose nodes are Riquier pre-rankings and edges are subsets of $\mathbb{N}_n$. Since Riquier pre-rankings on ΘU can be represented by real matrices of width $m+n$, this classification allows us to specify an arbitrary ranking by finitely many real-valued parameters (Rust and Reid, 1997, Theorem 29). This specification is not unique, and the construction of a unique specification is formulated as an open problem in Rust (1998).

In principle, the problem of construction of a ranking can be solved by directly applying the non-recursive description of rankings proposed in Rust and Reid (1997).[4]

Let $M_1, \ldots, M_n$ be non-singular *integer* matrices of size $m \times m$, in which every column is lexicographically greater than the zero column, let $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}^m$, and let σ be a permutation of $\mathbb{N}_n$. This data induces a ranking on $\mathbb{N}^m \times \mathbb{N}_n$ as follows.

[4] The author has learned this solution from private communication with Colin Rust.

Let t_{ij} be the number of rows, starting from the top, on which matrices M_i and M_j agree (i.e., the submatrices of M_i and M_j formed by the first t_{ij} rows are equal). For a vector $v \in \mathbb{Z}^m$ and $0 \le t \le m$, denote by $\pi_t(v)$ the vector consisting of the first t components of v. Define $(a, i) \le (b, j)$ if and only if either

$$\pi_{t_{ij}}(M_i a + \lambda_i) <_{\text{lex}} \pi_{t_{ij}}(M_j b + \lambda_j)$$

or

$$\pi_{t_{ij}}(M_i a + \lambda_i) = \pi_{t_{ij}}(M_j b + \lambda_j) \quad \text{and} \quad \sigma(i) \le \sigma(j).$$

According to Rust and Reid (1997, Theorem 29), $\le$ is a ranking; it is denoted

$$\le_{M_1,\dots,M_n,\lambda_1,\dots,\lambda_n,\sigma} \,. \tag{2}$$

By Rust and Reid (1997, Theorem 30), every finite set A contained in a ranking must be contained in a ranking of the form (2). In other words (Rust, 1998, Section 3.1), one can endow the set of all rankings with the minimal topology such that for all $(a, i), (b, j) \in \mathbb{N}^m \times \mathbb{N}_n$, the set

$$\{\le \ | \ (a, i) \le (b, j)\}$$

is open. Then rankings (2) will constitute a countable dense subset in the topological space of all rankings.

Now, since there are finitely many possible permutations σ and finitely many possibilities for the values t_{ij}, one can try them all; for each choice of σ and $\{t_{ij}\}$, one can check the existence of the corresponding integer matrices $M_1, \dots, M_n$ by solving a system of linear inequalities with rational coefficients, which is a linear programming problem. We leave out the details, since we are going to propose a more efficient algorithm.

7.1. Pre-rankings of finite type

A ranking on ΘU that can be extended to an admissible term order on $(\Delta \cup U)^\infty$ is called a *Riquier ranking* (Rust and Reid, 1997; Caboara and Silvestri, 1999).

Theorem 3 (*Rust and Reid, 1997, Theorem 6*). *For a Riquier ranking $\le$, there exists a positive integer s and an $s \times (m + n)$ real matrix M such that*

- *for $k = 1, \dots, m$, kth column c_k of M satisfies*
$$c_k \ge_{\text{lex}} (0, \dots, 0) \tag{3}$$
- $u \le v \iff M\phi(u) \le_{\text{lex}} M\phi(v)$.

Vice versa, any $s \times (m + n)$ real matrix M of rank $m + n$ satisfying (3) defines a Riquier ranking $\le_M$.

For a relation R, let R^{-1} denote the inverse relation, i.e.,

$$R^{-1} = \{(b, a) \mid (a, b) \in R\},$$

and let $R^* = R \cap R^{-1}$.

If the rank of the matrix M in the above theorem is less than $m + n$, then, by definition, M specifies a *Riquier pre-ranking* (Rust and Reid, 1997). In general, a *pre-ranking* is a relation P on

ΘU, which satisfies all axioms of a ranking, except for the antisymmetry condition: it is allowed that $(u, v) \in P^*$, $u \neq v$.

A Riquier pre-ranking P induces an equivalence relation $\approx_P$ on U:

$$u \approx_P v \quad \Longleftrightarrow \quad \exists\, \eta, \theta \in \Theta \;\; (\eta u, \theta v) \in P^*.$$

Let $U = U_1 \cup \cdots \cup U_q$ be the decomposition of U into equivalence classes w.r.t. $\approx_P$. Let P_l be a pre-ranking on ΘU_l, for each $1 \leq l \leq q$. We define a new pre-ranking $Q = P; \{P_1, \ldots, P_q\}$ as follows: $(\eta u, \theta v) \in Q$ if and only if $(\eta u, \theta v) \in P$ and

$$(\theta v, \eta u) \notin P \quad \text{or} \quad (\eta u, \theta v) \in P_{[u]},$$

where $[u] \in \{1, \ldots, p\}$ is the index of the equivalence class containing u. Clearly, in this definition one can equivalently write $P_{[v]}$ instead of $P_{[u]}$. Pre-ranking $Q = P; \{P_1, \ldots, P_q\}$ can be pictured as an unordered tree, in which P is the root and $P_1, \ldots, P_q$ are its children.

For two pre-rankings P and Q, we denote by $R = P; Q$ their sequential composition, i.e., the following pre-ranking: $(\eta u, \theta v) \in R$ if and only if $(\eta u, \theta v) \in P$ and

$$(\theta v, \eta u) \notin P \;\; \text{or} \;\; (\eta u, \theta v) \in Q.$$

Lemma 4. *If P and Q are Riquier pre-rankings, then so is their sequential composition.*

Proof. Given the matrices M_P and M_Q representing pre-rankings P and Q, one can see that the matrix

$$\begin{pmatrix} M_P \\ M_Q \end{pmatrix}$$

represents the ranking $P; Q$. $\square$

Definition 5 (*Rust and Reid, 1997*). A Riquier pre-ranking is called a pre-ranking of type 1.

A pre-ranking Q is *of type* $t > 1$, if t is minimal such that $Q = P; \{P_1, \ldots, P_q\}$, for some Riquier pre-rankings P and pre-rankings $P_1, \ldots, P_q$ of types $< t$.

Lemma 5. *In the above definition of pre-ranking Q of type t, the number l of equivalence classes w.r.t. $\approx_P$ is greater than* 1.

Proof. Suppose that $l = 1$. If P_1 is a Riquier ranking, then so is $Q = P; \{P_1\}$, which contradicts with the fact that Q is a pre-ranking of type $t > 1$.

If P_1 is a pre-ranking of type s, $1 < s < t$, then by definition it can be represented as $P_1 = R; \{R_1, \ldots, R_k\}$, where R_i are pre-rankings of type $< s$. By the previous lemma, $S = P; R$ is a Riquier pre-ranking. Moreover,

$$u \approx_S v \;\Rightarrow u \approx_R v.$$

In particular, this implies that each equivalence class V modulo $\approx_S$ is contained in an equivalence class U_i modulo $\approx_R$, where $1 \leq i \leq k$. Let R_V be the restriction of R_i to ΘV. Clearly, the type of R_V does not exceed that of R_i, i.e., $s - 1 \leq t - 2$. We obtain

$$Q = S; \{R_V\}_{V \in U/\approx_S},$$

where S is a Riquier pre-ranking and each R_V is a pre-ranking of type $\leq t - 2$. This contradicts the minimality of t. $\square$

Theorem 4 (*Rust and Reid, 1997, Theorem 18*). *Every ranking on ΘU is a pre-ranking of type $\leq n$.*

7.2. Satisfiability of a finite relation on partial derivatives by a ranking

Let A be a finite relation on ΘU. If A is empty, it is contained in any ranking. Otherwise, we proceed by induction on the number of elements in A, assuming that for all relations of size less than $|A|$ the problem of satisfiability by a ranking is solved.

Denote by $A\big|_U$ the projection of A on U:

$$(u, v) \in A\big|_U \iff \exists\, \eta, \theta \in \Theta \;\; (\eta u, \theta v) \in A.$$

Let $\approx_A$ be the reflexive symmetric transitive closure of $A\big|_U$; thus, $\approx$ is an equivalence relation on U. Let $U = U_1 \cup \cdots \cup U_p$ be the decomposition of U into equivalence classes w.r.t. $\approx_A$. Two cases are possible: $p > 1$ and $p = 1$.

Case $p > 1$ is easy. Let $A_k = A \cap (\Theta U_k)^2$, $1 \le k \le p$. For each k, we have $|A_k| < |A|$, hence by the inductive assumption the problem of satisfiability by a ranking is solved for A_k. Clearly, if A is contained in a ranking, then so is every A_k. Vice versa, if every A_k is contained in a ranking $\le_k$ on ΘU_k, then the following relation $\le$ is a ranking on ΘU and contains A:

$$\eta u \le \theta v \iff (u, v \in U_k \text{ and } \eta u \le_k \theta v) \text{ or } (u \in U_k,\; v \in U_l, \text{ and } k < l).$$

Case $p = 1$ is the interesting one. When $p = 1$, we have $u \approx_A v$ for all $u, v \in U$. We prove the following.

Lemma 6. *Let A be a finite relation on ΘU such that $u \approx_A v$ for all $u, v \in U$. If A is contained in a ranking, then there exist a pair $\tau \in A$ and a Riquier pre-ranking $R_\tau \supset A$ such that $\tau \notin R_\tau^*$.*

Proof. Assume that A is contained in a ranking $\le$; show the existence of τ and R_τ. According to Theorem 4, $\le$ is a pre-ranking of type $\le n$. Let P be the Riquier pre-ranking from the definition of a pre-ranking of type t (see Definition 5). By Lemma 5, not all $u, v \in U$ are equivalent w.r.t. the induced equivalence relation $\approx_P$.

We have that $\le$ contains A and is contained in P. Hence, $A \subset P$. Suppose that $A \subset P^*$. Then, for every pair $(\eta u, \theta v) \in A$, i.e., for all $u, v \in A\big|_U$, we have $(u, v) \in \approx_P$. Hence, the reflexive symmetric transitive closure of $A\big|_U$, which is $\approx_A$, is contained in $\approx_P$, which contradicts the fact that not all $u, v \in U$ are equivalent w.r.t. $\approx_P$. Hence, A is not contained in P^*, and we can take any $\tau \in A \setminus P^*$ and set $R_\tau = P$. $\square$

For a fixed $\tau \in A$, the existence of a Riquier pre-ranking R_τ satisfying the conditions of the above lemma can be effectively verified using the following generalization of Sturmfels (1995, Proposition 1.11), which is stated for admissible term orders (the proof in the case of Riquier rankings is identical, so we omit it).

Proposition 3. *Riquier pre-ranking R_τ exists iff the following system of linear inequalities has a solution $\vec{w} \in \mathbb{Q}^{m+n}$*

$$\begin{cases} \vec{w} \cdot \phi(u) < \vec{w} \cdot \phi(v), & (u, v) = \tau \\ \vec{w} \cdot \phi(u) \le \vec{w} \cdot \phi(v), & (u, v) \in A \setminus \{\tau\}. \end{cases}$$

If $\vec{w}$ exists, the single-row matrix $(\vec{w})$ specifies R_τ.

If it turns out that, for all $\tau \in A$, Riquier pre-ranking R_τ does not exist, then by Lemma 6, A is not contained in a ranking. Otherwise, we find a $\tau \in A$ and the corresponding R_τ using the above proposition. Let $A' = A \cap R_\tau^*$. Then $|A'| < |A|$, hence by the inductive assumption for

$|A'|$ the problem of computation of a ranking is solved. If A is contained in a ranking, then so is A'. Vice versa, if A' is contained in a ranking $\leq'$, then the ranking $R_\tau; \leq'$ contains A.

7.3. Example

We illustrate our algorithm on an example from Rust and Reid (1997). Let $\Delta = \{\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\}$, $U = \{u, v, w\}$, and

$$A = \{(u_x, u_y), (v_y, v_x), (v, u_y), (u, v_y), (w_x, w_{yy})\}.$$

Construct a ranking $\leq$ on ΘU containing A.

- Observation: $\leq$ cannot be a Riquier ranking, otherwise $u_x < u_y$ and $v_y < v_x$ would lead to a contradiction.
- Relation $\approx_A$ has two equivalence classes: $\{u, v\}$ and $\{w\}$.
- Consider class $\{w\}$, then a Riquier ranking R_1 on Θw containing $\{(w_x, w_{yy})\}$ is represented by the matrix

$$M_{R_1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

- Consider class $\{u, v\}$ and construct a ranking on $\Theta\{u, v\}$ containing

$$A_1 = \{(u_x, u_y), (v_y, v_x), (v, u_y), (u, v_y)\}.$$

- Does there exist a Riquier pre-ranking R_2 such that

$$(u_x, u_y) \in R_2 \setminus R_2^{-1}, \quad (v_y, v_x), (v, u_y), (u, v_y) \in R_2\ ?$$

  No, because $(v_y, v_x) \in R_2 \Rightarrow (u_y, u_x) \in R_2 \Rightarrow (u_x, u_y) \in R_2^{-1}$, contradiction.
- Does there exist a Riquier pre-ranking R_3 such that

$$(v_y, v_x) \in R_3 \setminus R_3^{-1}, \quad (u_x, u_y), (v, u_y), (u, v_y) \in R_3\ ?$$

  No, for the same reason.
- Does there exist a Riquier pre-ranking R_4 such that

$$(v, u_y) \in R_4 \setminus R_4^{-1}, \quad (u_x, u_y), (v_y, v_x), (u, v_y) \in R_4\ ?$$

  Yes, for example the one represented by the matrix $M_{R_4} = (1, 1, 0, 0)$.
- Let $A_2 = A_1 \cap R_4^* = \{(u_x, u_y), (v_y, v_x)\}$.
- There are two equivalence classes w.r.t. $\approx_{A_2}$: $\{u\}, \{v\}$.
- The Riquier rankings R_5 and R_6 on Θu and Θv containing $\{(u_x, u_y)\}$ and $\{(v_y, v_x)\}$ respectively are represented by matrices

$$M_{R_5} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad M_{R_6} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

A ranking $\leq$ containing A is defined as follows. For any pair of partial derivatives $t_1, t_2 \in \Theta U$, compare them according to the first applicable rule in the following list:

- Equivalence classes $\{u, v\}$ and $\{w\}$: $\Theta\{u, v\} < \Theta w$.

- Riquier ranking R_1: $w_x < w_{xx} < \cdots < w_y$.
- Riquier pre-ranking R_4: If $\theta_1, \theta_2 \in \Theta$ and $\operatorname{ord}\theta_1 < \operatorname{ord}\theta_2$, then $\theta_1\{u, v\} < \theta_2\{u, v\}$.
- Equivalence classes $\{u\}$ and $\{v\}$: $\theta_1 u < \theta_2 v$.
- Riquier ranking R_5: $u_x < u_{xx} < \cdots < u_y$.
- Riquier ranking R_6: $v_y < v_{yy} < \cdots < v_x$.

Clearly, each of the above rules corresponds to a Riquier pre-ranking, thus we can obtain a description of $\leq$ as a pre-ranking of finite type as well.

8. Conclusion and open problems

We have defined the concept of universal characteristic decomposition of a radical differential ideal and given a factorization-free algorithm for computing it. For a particular example of a radical differential ideal, the computation of the universal characteristic decomposition allowed us to easily detect a redundant component in the characteristic decomposition produced by the Rosenfeld–Gröbner algorithm, find a ranking for which the Rosenfeld–Gröbner algorithm produces an irredundant decomposition, and conclude that the ideal is universally characterizable.

It would be interesting to generalize the concept of Gröbner fan to radical differential ideals as well. For prime differential ideals, the Gröbner fan is uniquely defined and can be computed (Golubitsky, 2006b). It seems natural to define the Gröbner fan of a radical differential ideal as an intersection of the Gröbner fans of its essential prime components. However, it is not known whether essential prime components of a radical differential ideal can be computed (see the Ritt problem in Ritt (1950) and Kolchin (1973)). It may turn out that computing its Gröbner fan is an easier problem.

We hope that, similarly to the polynomial case, the concepts of differential Gröbner fan and universal characteristic decomposition will lead to efficient algorithms for decomposing radical differential ideals. It is particularly interesting to explore differential generalizations of the dynamic Buchberger algorithm (Caboara, 1993; Gritzmann and Sturmfels, 1993; Golubitsky, 2006a). In the polynomial case, choosing the optimal intermediate term orders appears to cause significant computational overhead. In the differential case, however, the intermediate coefficient swell is more rapid, which makes it worthwhile spending more time on choosing intermediate term orders, or even trying several term orders in parallel, in an attempt to avoid intermediate polynomials that are too large to be differentiated. Moreover, one can choose optimal rankings independently for each component of the radical differential ideal.

Among the more straightforward applications of the universal characteristic decomposition is the generalization of the Gröbner walk method to the case of radical differential ideals. The method has been generalized to prime differential ideals in Golubitsky (2004). It remains to be shown that an efficient transformation between the characteristic decompositions w.r.t. two rankings compatible with the same weight vector is possible. One can also try to avoid unnecessary splits of components during the walk, using the fact that a characteristic decomposition of the ideal is already known.

Acknowledgments

I am grateful to Carlo Traverso for the invitation to work in his research group at the University of Pisa and for financial support in 2004, at which time the idea of universal characteristic decomposition arose. I thank sincerely William Sit and Colin Rust for the invaluable discussions of rankings, and for comments and suggestions on the draft this paper. I highly appreciate the comments and useful references provided to me by Giuseppa Carrà Ferro, Hoon Hong, Évelyne Hubert, Marina Kondratieva, Alexey Ovchinnikov, Eugueny Pankratiev, Greg Reid, Michael Singer, Allan Wittkopf, Alexey Zobnin, and the anonymous referees.

The author was partially supported by the Progetto di Interesse Nazionale "Algebra Commutativa e Computazionale" of the Italian "Ministero dell'Istruzione dell'Università della Ricerca Scientifica Tecnologica, RFBR grant no. 02-01-01033, and NSERC grant PDF-301108-2004.

References

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1999. Computing representations for radicals of dinitely generated differential ideals. Tech. report, LIFL.

Boulier, F., Lemaire, F., 2000. Computing canonical representatives of regular differential ideals. In: ISSAC'00: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation. ACM Press, New York, NY, USA, pp. 38–47. http://hal.archives-ouvertes.fr/hal-00139177.

Caboara, M., 1993. A dynamic algorithm for Gröbner basis computation. In: Proc. ISSAC'93. pp. 275–283.

Caboara, M., Silvestri, M., 1999. Classification of compatible module orderings. J. Pure Appl. Algebra 142, 13–24.

Carrà Ferro, G., Sit, W., 1994. On term-orderings and rankings. In: Lecture Notes in Pure and Applied Mathematics. Computational Algebra 151, 31–77.

Collart, S., Kalkbrener, M., Mall, D., 1993. The Gröbner walk. Tech. report, Swiss Federal Inst. of Tech.

Fukuda, K., Jensen, A., Lauritzen, N., Thomas, R., 2007. The generic Gröbner walk. J. Symbolic Comput. 42, 298–312.

Golubitsky, O., 2004. Gröbner walk for characteristic sets of prime differential ideals. In: Ganzha, V., Mayr, E., Vorozhtsov, E. (Eds.), Proc. 7th Workshop on Comp. Alg. in Sc. Comp. TU München, Germany, pp. 207–221.

Golubitsky, O., 2006a. Converging term order sequences and the dynamic Buchberger algorithm. Preprint.

Golubitsky, O., 2006b. Gröbner fan and universal characteristic sets of prime differential ideals. J. Symbolic Comput. 41 (10), 1091–1104.

Golubitsky, O., Kondratieva, M., Ovchinnikov, A., 2007. Algebraic transformation of differential characteristic decompositions from one ranking to another. Preprint.

Gritzmann, P., Sturmfels, B., 1993. Minkowski addition of polytopes: Computational complexity and applications to Gröbner bases. SIAM J. Discrete. Math. 6 (2), 246–269.

Hubert, E., 2000. Factorization-free decomposition algorithms in differential algebra. J. Symbolic Comput. 29, 641–662.

Hubert, E., 2003a. Notes on triangular sets and triangulation–decomposition algorithms I: Polynomial systems. In: Symbolic and Numerical Scientific Computing 2001. pp. 1–39.

Hubert, E., 2003b. Notes on triangular sets and triangulation–decomposition algorithms II: Differential systems. In: Symbolic and Numerical Scientific Computing 2001. pp. 40–87.

Kolchin, E., 1973. Differential Algebra and Algebraic Groups. Academic Press.

Kondratieva, M., Levin, A., Mikhalev, A., Pankratiev, E., 1999. Differential and Difference Dimension Polynomials. Klüver publishers.

Kondratieva, M., Ovchinnikov, A., 2004. On computing characteristic sets of arbitrary radical differential ideals. In: Proc. ACA 2004. pp. 38–48.

Mora, T., Robbiano, L., 1988. The Gröbner fan of an ideal. J. Symbolic Comput. 6, 183–208.

Ritt, J., 1950. Differential Algebra. Dover.

Rust, C., 1998. Rankings for derivatives for elimination algorithms and formal solvability of analytic partial differential equations. Ph.D. Thesis, University of Chicago.

Rust, C., Reid, G., 1997. Rankings of partial derivatives. In: Proc. ISSAC'97. Kihei, Maui, Hawaii, United States, pp. 9–16.

Sturmfels, B., 1995. Gröbner Bases and Convex Polytopes. In: University Lecture Series, vol. 8. American Mathematical Society.

Tran, Q.-N., 2000. A fast algorithm for gröbner basis conversion and its applications. J. Symbolic Comput. 30, 451–467.